

Serial No. 09/829,674

Page 8 of 12

REMARKS

Claim 2 has been canceled. Claims 1 and 3-10 remain pending in the present application. Applicant amends claims 1 and 7-10 for clarification. Applicant refers to Figs. 10 and 13-20, and their corresponding description in the specification for exemplary embodiments of and support for the claimed invention. No new matter has been added.

Claim 10 is rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,373,950 to Rowney in view of "Handbook of Applied Cryptography" by Menezes et al. and further in view of U.S. Patent No. 6,718,274 to Huang et al.; claims 1-2 and 4-9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney in view of U.S. Patent No. 6,732,269 to Baskey et al. and Menezes et al. and further in view of Huang et al.; and claim 3 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney in view of Baskey et al., Menezes et al., Huang et al. and U.S. Patent No. 6,351,813 to Mooney et al. Applicant amends independent claims 1 and 7-10 in a good faith effort to further clarify the invention as distinguished from the cited references, and respectfully traverses the rejections.

The Examiner cited Fig. 1B of Rowney as alleged disclosure of the claimed feature of authenticating a direct communication between a user terminal and an electronic market server. Applicant respectfully submits, however, that the cited figure of Rowney merely illustrates a direct authentication and communication between customer 120 and merchant 130. Thus, the proposed combination of references would still only have suggested directly authenticating each communication link, and would not have suggested the claimed feature of authenticating a direct communication using a proxy therebetween.

84158287_1.DOC

Serial No. 09/829,674

Page 9 of 12

Again, the Examiner acknowledged that Rowney does not disclose “the proxy server being provided between a user terminal and an electronic market server and the shared key being a common key,” (page 5, lines 17-19 of the Office Action) and relied upon Baskey et al. as a combining reference for disclosing a proxy server between a client and a server, and relied upon Menezes et al. as a further combining reference for disclosing a common key. The cited portions of Baskey et al., col. 5, lines 17-37, merely describe an SSL proxy server operable in routing client specific SSL connections onto a persistent secure connection between the SSL proxy server and a transaction server. And the cited portions of Menezes et al., provide overviews of symmetric-key encryption (also known as single-key, one-key, private key, and conventional encryption), and “key-encrypting keys.”

Therefore, the cited portions of Baskey et al. only describe an SSL proxy server that is a communication proxy for a client to a transaction server. And a combination of such portions of Baskey et al. with the cited portions of Rowney—including Fig. 1B thereof—would still have only suggested such an SSL proxy server that routes client specific SSL connections onto a persistent secure connection between the SSL proxy server itself and a transaction server. In other words, each of the cited references only describe directly authenticating each communication link, and none suggest the claimed feature of authenticating a direct communication between a user terminal and an electronic market server using a proxy therebetween.

The Examiner cited Huang et al. as a new combining reference that allegedly discloses the claimed home card feature. The cited portions of Huang et al. describe the use of smart cards

84158287_1.DOC

Serial No. 09/829,674

Page 10 of 12

for protecting private keys, isolating security-critical calculations, etc. This reference would, thus, still have failed to cure the above-described deficiencies of the cited references.

As such, even assuming, arguendo, that it would have been obvious to one skilled in the art to combine Rowney, Baskey et al., Menezes et al., and Huang et al., the combination would have, at most, suggested a persistent secure connection between the SSL proxy server and a transaction server, as described in Baskey et al., through which communication from a user terminal is conducted. Such a combination would, thus, still fail to disclose or suggest, “an encrypted communication is executed directly between the user terminal and the electronic market server by using the common key X that was exchanged between the proxy server and the electronic market server,” as claimed.

Furthermore, none of the cited references disclose or suggest the claimed feature of a home card at a proxy server and an access card at a user terminal cooperating to establish an encrypted communication session and to exchange the common key X’.

As such, even assuming, arguendo, that it would have been obvious to one skilled in the art to combine Rowney, Baskey et al., Menezes et al., and Huang et al., such a combination would still have failed to teach or suggest,

“[a] proxy server, provided between a user terminal and an electronic market server, including a proxy facility for executing authentication and encryption to the electronic market server, instead of the user terminal, in an electronic commercial transaction, comprising:

an establishing means for establishing an encrypted communication session between the user terminal and the proxy server, using public and secret keys of the user terminal and an electronic signature both transmitted from the user terminal;

a proxy means for executing authentication of a certificate and exchanging a common key X between the proxy server and the

84158287_1.DOC

Serial No. 09/829,674

Page 11 of 12

electronic market server, using public and secret keys of the electronic market server;

an informing means for informing the common key X to the user terminal through the encrypted communication session, which common key X is encrypted by using a common key X' that is exchanged between the user terminal and the proxy server; and

a home card including an encryption managing means for executing the electronic signature and authentication of the certificate in order to execute authentication and exchange of the common key to the electronic market server, said home card cooperating with an access card connected to said user terminal to establish said encrypted communication session and to exchange said common key X',

whereby an encrypted communication is executed directly between the user terminal and the electronic market server by using the common key X that is exchanged between the proxy server and the electronic market server," as recited in claim 1. (Emphasis added)

Accordingly, Applicant respectfully submits that independent claim 1, together with claims 4-6 dependent therefrom, is patentable over Rowney, Baskey et al., Menezes et al., Huang et al., separately and in combination. Independent claims 7-10 incorporate features that correspond to those of claim 1 cited above, and are, therefore, patentable over the cited references for at least the same reasons.

Again, the cited portions of Mooney et al., col. 1, lines 59-67, col. 2, lines 1-11, and col. 9, lines 31-36, describe the use of a user smart card for access control, the use of a secret password for decrypting encrypted data transferred from a first site to a second site, and the use of a second password or biometric information to generate an encryption key. Such portions, therefore, do not teach or suggest the above-cited features of claim 1, including the claimed feature of a home card at a proxy server and an access card at a user terminal cooperating to establish an encrypted communication session and exchange the common key X'. Applicant, therefore, respectfully submits that the combination of Mooney et al. with Rowney, Baskey et
84158287_1.DOC

Serial No. 09/829,674

Page 12 of 12

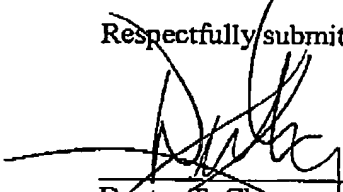
al., Menezes et al., and Huang et al. would not have taught or suggested the above features of claim 1 that are incorporated in dependent claim 3, even assuming such a combination would have been obvious to one skilled in the art. Accordingly, Applicant submits that claim 3 is patentable over Rowney, Baskey et al., Menezes et al., Huang et al., and Mooney et al. for at least the above-stated reasons with respect to claim 1, from which it depends.

Statements appearing above in respect to the disclosures in the cited references represent the present opinions of the undersigned attorney and, in the event that the Examiner disagrees with any of such opinions, it is respectfully requested that the Examiner specifically indicate those portions of the respective reference providing the basis for a contrary view.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,



Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11683 (FUJA 18.570)
DTC:bf

84158287_1.DOC